UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

SYMANTEC CORPORATION,

Plaintiff,

v.

CASE NO. 02-CV-73740-DT
CHIEF JUDGE BERNARD A. FRIEDMAN
MAGISTRATE JUDGE PAUL KOMIVES

COMPUTER ASSOCIATES INTERNATIONAL, INC.,

Defendant.
_____/

REPORT AND RECOMMENDATION ON COMPUTER ASSOCIATES' MOTIONS FOR SUMMARY JUDGMENT OF NO INFRINGEMENT (docket #118, 119 & 121)

I. RECOMMENDATION: The Court should grant CA's motions for summary judgment of no infringement with respect to the accused EAV/ARCserve and Intrusion Detection products, and deny CA's motion for summary judgment of no infringement with respect to the accused Content Inspection products. Specifically, the Court should:

(1) conclude that there are no genuine issues of material fact with respect to whether the accused EAV and ARCserve products screen the data while it is being transferred or while the computer is receiving the data, and that there are no genuine issues of material fact with respect to whether the EAV products cause a transfer of digital data. Accordingly, the Court should grant CA's motion for summary judgment of no infringement with respect to the accused EAV and ARCserve products (docket #118);

(2) conclude that Symantec has raised genuine issues of material fact with respect to whether the accused Content Inspection products infringe the patent both literally and under the doctrine of equivalents. Accordingly, the Court should deny CA's motion for summary judgment of non-infringement with respect to the Content Inspection products (docket #119); and

(3) conclude that there are no genuine issues of material fact with respect to whether the accused Intrusion Detection product screens data "prior to storage," "automatically inhibits the storage of data," or "causes a quantity of digital data to be transferred." Accordingly, the Court should grant CA's motion for summary judgment of non-infringement with respect to the Intrusion Detection product (docket #121).

II. REPORT:

A. *Background*

In this patent infringement suit, plaintiff Symantec Corporation ("Symantec" or "plaintiff")

alleges that products of defendant Computer Associates International, Inc. ("CA" or "defendant"), infringe on its rights under U.S. Patent No. 5,319,776 ("the '776 patent"). Currently pending before the Court are nine motions for summary judgment filed by the parties.[1] This Report addresses the three motions for summary judgment of non-infringement filed by Computer Associates. The remaining motions are addressed in separate Reports being filed on this date.

As explained in my Opinion and Order construing the patent claims, the '776 patent was issued on June 7, 1994, and is entitled "In Transit Detection of Computer Virus with Safeguard." The patent discloses twenty method claims, two of which, Claims 1 and 18, are independent claims and the remainder of which are dependent claims. As briefly described by the Federal Circuit in a prior case involving the '776 patent, "[t]he claimed invention scans a body of data during its transfer, *i.e.*, before storage of the data with potential viruses on the destination storage medium. If the program detects signs of a virus during the scan, the program automatically blocks storage." *Hilgraeve Corp. v. McAfee Assocs., Inc.*, 224 F.3d 1349, 1350 (Fed. Cir. 2000) (*Hilgraeve I*); *see also*, *Hilgraeve Corp. v. Symantec Corp.*, 265 F.3d 1336, 1339 (Fed. Cir. 2001) (*Hilgraeve II*).

On November 9, 2004, CA filed these three motions for summary judgment on the issue of infringement. In the motions, CA argues that there is no genuine issue of material fact with respect

---

[1]The nine pending motions, all filed on November 9, 2004, are: (1) defendant's motion for summary judgment on unenforceability due to inequitable conduct (docket #113); (2) defendant's motion for summary judgment of laches (docket #114); (3) plaintiff's motion for summary judgment on defendant's defenses of laches, implied licence, waiver, and equitable estoppel (docket #115); (4) plaintiff's motion for summary judgment that Richard B. Levin is not an inventor (docket #116); (5) plaintiff's motion for summary judgment of no inequitable conduct (docket #117); (6) plaintiff's motion for summary judgment of no invalidity (docket #120); and (7-9) defendant's three motions for summary judgment on infringement with respect to three separate products which are the subject of plaintiff's infringement claims (docket #118, 119 & 121).

to whether three groups of its accused products– (1) Etrust, Etrust EZ, and ARCserve; (2) Content Inspection products; and (3) Intrusion Detection products–infringe the patent. CA argues that each of these groups of products fails to meet several of the claim limitations, and thus do not literally infringe the patent. CA also argues that the products do not infringe under the doctrine of equivalents, and that Symantec is estopped from asserting infringement on the basis of equivalents. On December 1, 2004, Symantec filed, under seal, responses to each of these motions. CA filed replies on December 20, 2004. Following the Court's construction of the claims, the parties filed supplemental briefs. For the reasons that follow, the Court should grant CA's motions for summary judgment of no infringement with respect to the EAV/ARCserve products and the Intrusion Detection product, and deny CA's motion for summary judgment with respect to the Content Inspection products.

B. *Legal Standard*

Any appeal from the Court's judgment in this case lies exclusively in the United States Court of Appeals for the Federal Circuit. *See* 28 U.S.C. § 1295(a)(1). Accordingly, this Court is bound by the jurisprudence of the Federal Circuit as to those matters which relate to the Federal Circuit's exclusive jurisdiction. *See Kudlacek v. DBC, Inc.*, 115 F. Supp. 2d 996, 1019 (N.D. Iowa 2000); *Sample v. United States*, 838 F. Supp. 373, 375 (N.D. Ill. 1993) ("United States Court of Appeals, Federal Circuit, jurisprudence controls since the case would be appealed to the Federal Circuit."), *aff'd*, 65 F.3d 939 (Fed. Cir. 1995). However, the general standards governing summary judgment are controlled by the law of the regional circuit court–here the Sixth Circuit. *See Parental Guide of Tex., Inc. v. Thomson*, 446 F.3d 1265, 1268 (Fed. Cir. 2006); *Microstrategy Inc. v. Business Objects, S.A.*, 429 F.3d 1344, 1349 (Fed. Cir. 2005).

Under Rule 56, summary judgment should be granted "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue of material fact and that the moving party is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c). "An issue of fact is 'genuine' if the evidence is such that a reasonable jury could return a verdict for the non-moving party." *Hedrick v. Western Reserve Care Sys.*, 355 F.3d 444, 451 (6th Cir. 2004) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). "A fact is material only if its resolution will affect the outcome of the lawsuit." *Hedrick*, 355 F.3d at 451-52 (citing *Anderson*, 477 U.S. at 248). In deciding a motion for summary judgment, the Court must view the evidence in a light most favorable to the non-movant as well as draw all reasonable inferences in the non-movant's favor. *See Sutherland v. Michigan Dep't of Treasury*, 344 F.3d 603, 613 (6th Cir. 2003); *Rodgers v. Banks*, 344 F.3d 587, 595 (6th Cir. 2003).

The moving party's initial burden differs depending on whether the non-movant or the movant bears the ultimate burden of proof on the issue on which summary judgment is sought. In the former case, "[t]he moving party has the initial burden of showing the absence of a genuine issue of material fact as to an essential element of the non-moving party's case." *Hedrick*, 355 F.3d at 451 (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986)). To meet this burden, the moving party need not produce evidence showing the absence of a genuine issue of material fact. Rather, "the burden on the moving party may be discharged by 'showing' -- that is, pointing out to the district court -- that there is an absence of evidence to support the non-moving party's case." *Celotex Corp.*, 477 U.S. at 325. "Once the moving party satisfies its burden, 'the burden shifts to the nonmoving party to set forth specific facts showing a triable issue.'" *Wrench LLC v. Taco Bell Corp.*, 256 F.3d 446, 453 (6th Cir. 2001) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio*

Corp., 475 U.S. 574, 587 (1986)); *see also*, FED. R. CIV. P. 56(e).

However where "the crucial issue is one on which the movant will bear the ultimate burden of proof at trial, summary judgment can be entered only if the movant submits evidentiary materials to establish all of the elements of the claim or defense." *Stat-Tech Liquidating Trust v. Fenster*, 981 F. Supp. 1325, 1335 (D. Colo. 1997); *see also, United States v. Four Parcels of Real Property*, 941 F.2d 1428, 1438 (11th Cir. 1991); *Resolution Trust Corp. v. Gill*, 960 F.2d 336, 340 (3d Cir. 1992). In other words, in such a case the movant "must satisfy both the initial burden of production on the summary judgment motion–by showing that no genuine dispute exists as to any material fact–and the ultimate burden of persuasion on the claim–by showing that it would be entitled to a directed verdict at trial." William W. Schwarzer, et al., *The Analysis and Decision of Summary Judgment Motions*, 139 F.R.D. 441, 477-78 (1991). "Once a moving party with the burden of proof makes such an affirmative showing, it is entitled to summary judgment unless the non-moving party comes forward with probative evidence that would demonstrate the existence of a triable issue of fact." *In re Bressman*, 327 F.3d 229, 238 (3d Cir. 2003).

To create a genuine issue of material fact, however, the non-movant must do more than present some evidence on a disputed issue. As the Supreme Court has explained:

> There is no issue for trial unless there is sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party. If the [non-movant's] evidence is merely colorable, or is not significantly probative, summary judgment may be granted.

Anderson, 477 U.S. at 249-50. (citations omitted); *see Celotex Corp.*, 477 U.S. at 322-23; *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986). Thus, "[t]he existence of a mere scintilla of evidence in support of the non-moving party's position will not be sufficient; there must be evidence on which the jury could reasonably find for the non-moving

party." *Sutherland*, 344 F.3d at 613.

C. *Infringement Generally*

A patent may be infringed in one of two ways–literally or by equivalents. "Literal infringement of a claim occurs when every limitation recited in the claim appears in the accused device, *i.e.*, when 'the properly construed claim reads on the accused device exactly.'" *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1358 (Fed. Cir. 2000) (quoting *Amhil Enters., Ltd. v. Wawa, Inc.*, 81 F.3d 1554, 1562 (Fed. Cir. 1996)). Infringement under the doctrine of equivalents occurs when "the accused product contain[s] each limitation of the claim or its equivalent." *Id.*; *see also, Warner-Jenkinson Co., Inc. v. Hilton-Davis Chem. Co.*, 520 U.S. 17, 40 (1997). Thus, in order to succeed on its infringement claims, Symantec must "show the presence of *every* element or its substantial equivalent in the accused device." *Elekta Instrument S.A. v. O.U.R. Scientific Int'l, Inc.*, 214 F.3d 1302, 1306 (Fed. Cir. 2000) (emphasis added). Further, because a dependent claim necessarily contains each limitation of the independent claim to which it is attached, a finding of no infringement on an independent claim compels a finding of no infringement on the dependent claims. *See Hoffer v. Microsoft Corp.*, 405 F.3d 1326, 1331 (Fed. Cir. 2005); *Minnesota Mining & Mfg. Co. v. Chemque, Inc.*, 303 F.3d 1294, 1300 (Fed. Cir. 2002). "Whether the accused device contains each claim element exactly or its equivalent is a question of fact," *KCJ Corp.*, 223 F.3d at 1355, and Symantec's burden here is to demonstrate a genuine issue of fact with respect to whether the accused products contain each element of the claims of the '776 patent.

D. *Prosecution History Estoppel*

With respect to each group of accused products, CA argues, *inter alia*, that it is entitled to summary judgment on the issue of infringement by equivalents because Symantec is estopped based

on the prosecution history of the '776 patent. Symantec responds that it is barred from asserted equivalents with respect to products that do not screen prior to storage. As the Supreme Court has explained, a limitation inserted specifically to avoid a prior art determination by the PTO acts as a limit on the claim for purposes of infringement analysis. *See Warner-Jenkinson Co., Inc. v. Hilton-Davis Chem. Co.*, 520 U.S. 17, 30-33 (1997). Thus, "[i]f claim scope is relinquished during prosecution on grounds of patentability, the doctrine of prosecution history estoppel provides that the relinquished scope can not be recovered" in an infringement action. *Merck & Co., Inc. v. Mylan Pharm., Inc.*, 190 F.3d 1335, 1340 (Fed. Cir. 1999); *see also, Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd.*, 535 U.S. 722, 733-34 (2002); *Bai v. L & L Wings, Inc.*, 160 F.3d 1350, 1355 (Fed. Cir. 1998).

The Federal Circuit has already considered this issue, and its decision is binding here under principles of *stare decisis*. In *Hilgraeve I* the Court explained:

> As originally submitted, the application that led to the '776 patent did not contain claim 18. Claim 18 was added in the applicant's first response to rejection of all its claims. In this response, the applicant stated to the examiner that "[t]he present invention also has the capability to respond to the detection of a virus by *not only* preventing the copying of the complete file, but also . . . ." (Emphasis added.) In other words, the applicant was stating that when the scanning program detected a virus, it prevented the copying of the complete file (among other things). Because an incomplete file would not be "sufficiently present on the destination storage medium, and accessible by the operating system or other programs" (except perhaps for erasure), the patentee may not now assert equivalents to claim 18 that allow screening after storage. *See Hilgraeve*, 70 F.Supp.2d at 748-50. Claim 1 acquired the phrase "prior to storage on the destination storage medium" in a later amendment, after which the patent was granted. Hilgraeve admits that it amended its claims to specify screening "prior to storage" to procure its patent. A surrender of subject matter during patent prosecution may preclude recapturing any part of that subject matter, even if it is equivalent to the matter expressly claimed. *See Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 117 S.Ct. 1040, 1044, 137 L.Ed.2d 146 (1997). In other words, prosecution history estoppel bars recapture of subject matter surrendered during prosecution. By limiting the added claim 18 to screening before storage, and specifically adding "screening . . . prior to storage" to

> claim 1, Hilgraeve surrendered the possibility of infringement by equivalence of any process that does not contain this modification, i.e., that screens after storage.

Hilgraeve I, 224 F.3d at 1355. Thus, Symantec is precluded from asserting infringement by equivalence with respect to the "screening prior to storage" elements of Claims 1 and 18, and therefore must show that the accused devices literally infringe these elements. With respect to the other elements of the patent claims, Symantec is free to argue that the accused products embody the patent claims either literally or by equivalents.

E. *Etrust, Etrust EZ, and ARCserve*

CA first contends that it is entitled to summary judgment with respect to his Etrust and Etrust EZ products (together "EAV products"), as well as with respect to its ARCserve program. The Court should grant CA's motion.

1. *The Accused Products*

The EAV products, according to CA, are desktop antivirus programs that run on a computer system and protect that system from viruses. *See* CA's eTrust Br., Ex. 3, Decl. of Benjamin Goldberg, ¶ 11. According to CA's expert, "EAV can employ two scanning modes: (a) after the file is closed; or (b) when the file is opened." *Id*. He further explains that, under either the outgoing scan ("scan on open") or the incoming scan ("scan-after-close"), the EAV products scan only files that have been completely written to the destination storage medium. *See id*., ¶¶ 12-13. According to Goldberg,

> When EAV is invoked, it accesses the file stored on disk . . . , reads selected portions of the file into the computer's memory, and on the basis of the selected portions of the filed read into memory, determines whether a virus is present. If a virus is found, it may be cured, or the file may be deleted. If no virus is found, or if the virus is cured, the file is allowed to remain on the destination storage medium.

Id., ¶ 16.

With respect to ARCserve, Professor Goldberg explains:

> ARCserve is archive software designed to backup and restore data. Only the restore function of ARCserve is accused of infringing the '776 patent. The restore function reads files from backup media and can restore those files to a computer system having a destination storage medium, such as a hard disk drive. Once a file is restored to the destination storage medium, ARCserve checks the file to determine whether it has a virus. If a virus is detected, ARCserve can delete the file containing the virus. For the purpose of this declaration, ARCserve operates in the same manner as EAV, except that ARCserve acts as the copy or download program, and thus ARCserve causes the transfer of digital data from the source storage medium.

Id., ¶ 17.[2]

CA contends that EAV and ARCserve fail to embody a number of limitations of independent Claim 1 and its dependent Claims 2-11, 13-14, and 16-17, as well as those of independent Claim 18 and its dependent Claims 19-20.

2. *"A Method of Screening the Data as It Is Being Transferred" and "Searching . . . while Said Computer is Receiving a Stream of Digital Data*

Claim 1 of the patent describes a "method of screening the data as it is being transferred." Although set out in the preamble, in its claim construction the Court concluded that this language is a limitation on the patent claims and that the phrase means "a method of screening the data while it is being moved or copied and before the data is stored to the computer storage medium." Opinion and Order, dated 3/16/05, at 15 (footnote omitted). Similarly, Claim 18 requires the program search for a plurality of virus signatures while the computer is receiving a stream of digital data. The parties' principle dispute with respect to the EAV and ARCserve programs, as they relate to these

---

[2]This description of the accused product is based on the opinion of CA's expert, and thus is disputed in some respects by Symantec. Professor Goldberg's declaration is quoted here merely to provide a basic understanding of the software, and not to resolve any of the infringement issues discussed below. It is not to be taken as resolving, or suggesting a resolution of, any of the issues raised by the parties.

limitations, focuses on the relationship between these limitations and the Court's construction of "storage." CA argues that a quantity of data can be written to the destination storage medium and therefore no longer be in transit–*i.e.*, no longer being moved or copied–even if it is not "stored" as that phrase is used in the patent. CA argues that because "storage" occurs when the data is both written to the destination storage medium and accessible to the operating system, it is possible for the data to be written to the storage medium such that it is no longer being moved or copied, but is not yet stored. Under this view of the relationship between the patent terms, CA argues that the EAV and ARCserve programs do not embody the limitation of being scanned while the file is being moved or copied, or while the computer is receiving the stream of data. Symantec argues that CA is attempting to undo the Court's claim construction. Because the Court explicitly substituted "stored" for "written" in CA's proposed definition of the preamble language, *see* Opinion & Order, dated 3/16/05, at 15 n.7, Symantec argues that data is still in-transit so long as it has not been "stored" within the meaning of the patent.

While the Court did substitute "stored" for "written" in CA's proposed definition, this alone does not answer the pertinent question. The Court's construction–"a method of screening the data while it is being moved or copied and before the data is stored to the computer storage medium"–can be read in two ways.[3] As Symantec argues, it could be read to mean that anything occurring before storage constitutes "being moved or copied;" that is, it could be read that the phrase occurring after the "and" merely defines the phrase occurring before the "and." On the contrary, as CA argues, it is equally permissible to view the construction as imposing two separate requirements: that the

[3]Importantly, the Court expressly declined to consider in its claim construction whether its construction of the phrase "adds any limitation which is not already encompassed by other terms in the claims." Opinion & Order, dated 3/16/05, at 15.

screening occur both (a) while the data is in transit and (b) before storage. The Court should adopt CA's argument and reject that of Symantec.

Adopting Symantec's argument would essentially read out of the patent the in-transit limitations in Claims 1 and 18. Under Symantec's construction in-transit merely equals "prior to storage." However, nothing in the patent itself, or in any evidence submitted by the parties, indicates that "as [the data] is being transferred" and "while the computer is receiving" mean simply that the data has not been "stored." If they did, there would have been no reason to add these limitations during the prosecution of the patent–and there would have been no need for Symantec to vigorously argue in its claim construction brief that this preamble language does not constitute a claim limitations–since the claims as originally drafted already required screening prior to storage. As the Federal Circuit has repeatedly explained, "[a]ll limitations in a claim must be considered meaningful." *Lantech, Inc. v. Keip Mach. Co.*, 32 F.3d 542, 546 (Fed. Cir. 1994); *accord Unique Concepts, Inc. v. Brown*, 939 F.2d 1558, 1562 (Fed. Cir. 1991); *Perkin-Elmer Corp. v. Westinghouse Elec. Corp.*, 822 F.2d 1528, 1532-33 (Fed. Cir. 1987). Thus, a court "err[s] as a matter of law by effectively reading out a specific and clearly stated limitation[.]" *Lantech*, 32 F.3d at 547. To equate "being transferred" and "while receiving" with "prior to storage" would leave the former limitations with no effect whatsoever.

Under this view, there are no genuine issues of material fact with respect to whether the ARCserve and EAV products infringe the patent. Professor Goldberg declares that the programs do not screen the data as it is being transferred, but only do so after the data has stopped moving and is physically present, in its entirety, on the destination storage medium. *See* CA's eTrust Supp. Br., Ex. 21, Supp. Decl. of Benjamin Goldberg, ¶ 18. To rebut this claim, Symantec presents the

declaration of its expert, David Klausner, who opines that the EAV products scan during transfer because the products "trap" the creation of a new file while receiving data and marks the file as "dirty" before the data is written to the storage medium. *See* Symantec's eTrust Br., Ex. 3, Decl. of David Klausner, ¶ 18; *see also, id*., Ex. 5, Dep. Tr. of John Gargiulo, at 68. Klausner also opines that this marking constitutes the first step in the scanning process, and thus the scanning begins while the data is in transit. *See id*., Ex. 3, Decl. of David Klausner, ¶ 18. However, as CA correctly notes, the screening process described in the patent requires a search of the incoming data for predefined virus sequences. Symantec has provided no evidence to suggest that simply marking a file for later searching itself constitutes a part of the search, and the ordinary understanding of "search" does not admit such a construction. Accordingly, the Court should conclude that there are no genuine issues of material fact with respect to whether the EAV and ARCserve products scan data "while it is being transferred" and "while the computer is receiving" the data.

3. *"Causing a Quantity of Digital Data To Be Transferred"*

Additionally, the Court should conclude that the EAV products do not cause a transfer of digital data, and thus do not infringe Claim 1 and its dependent claims. CA also argues that its EAV products do not "cause[] a quantity of digital data to be transferred." Rather, CA argues, the transfer of data is caused by a separate downloading or copying program, and thus its EAV products cannot infringe Claim 1 or its dependent claims.[4] In support, CA relies on the declaration of its expert, Benjamin Goldberg, who declares that "the transfer of data from the source storage medium is caused by a downloading or copying program. While a user may be able to command or request a

[4]For purposes of this motion, CA concedes that the ARCserve product does cause a transfer of digital data. *See* CA's eTrust Supp. Br., Ex. 21, Supp. Decl. of Benjamin Goldberg, ¶ 17.

downloading or copying program to transfer data from a source computer to the user's computer, it is not possible for a user to command or request the EAV software to initiate such a transfer." CA's eTrust Supp. Br., Ex. 13, Supp. Decl. of Benjamin Goldberg, ¶ 21. Symantec does not dispute this assertion, but rather argues that CA promotes its product to be used in an infringing manner with the downloading or copying program, and thus is liable for inducing infringement under 35 U.S.C. § 271(b). The Court should disagree.

Under § 271, "[w]hoever actively induces infringement of a patent shall be liable as an infringer." 35 U.S.C. § 271(b). To establish inducement of infringement, Symantec must show two elements. First, Symantec must show direct infringement on the part of someone. "It is well settled that there can be no inducement of infringement without direct infringement by some party. Upon a failure of proof of direct infringement, any claim of inducement of infringement also fails." *Epcon Gas Sys., Inc. v. Bauer Compressors, Inc.*, 279 F.3d 1022, 1033 (Fed. Cir. 2002) (citation omitted); *see also, Alloc, Inc. v. International Trade Comm'n*, 342 F.3d 1361, 1374 (Fed. Cir. 2003) (direct infringement "is a prerequisite to indirect infringement."); *Met-Coil Sys. Corp. v. Korners Unlimited, Inc.*, 803 F.2d 684, 687 (Fed Cir. 1986) ("Absent direct infringement of the patent claims, there can be . . . no[] inducement of infringement."). "[A] patentee must show that an alleged infringer knowingly induced another to commit an infringing act to establish inducement under section 271(b)." *Alloc*, 342 F.3d at 1374. That is, "the accused infringer must be shown to have had actual knowledge of the patent and the actual intent to induce infringement." *Young Dental Mfg. Co. v. Q3 Special Prods., Inc.*, 891 F. Supp. 1345, 1348 (E.D. Mo. 1995). Thus, "'sale of a lawful product by lawful means, with the knowledge that an unaffiliated, third party may infringe, cannot, in and of itself, constitute inducement of infringement.'" *Dynacore Holdings Copr. v. U.S. Philips Corp.*,

363 F.3d 1263, 1276 n.6 (Fed. Cir. 2004) (quoting *Organon Inc. v. Teva Pharms., Inc.*, 244 F. Supp. 2d 370, 380 (D.N.J. 2002)).

Here, Symantec has offered nothing to show that any third party has infringed the '776 patent through the use of the EAV products. Symantec's inducement argument derives from Goldberg's admission that software used with the EAV programs cause such transfers to take place. This admission, however, does not establish that the "causing" step is performed by the EAV products, rather than the additional software. Symantec's inducement argument can be sustained only if a separate program causing the transfer of data is an equivalent to the "causing" limitation of the patent. Such an equivalence finding, however, would effectively vitiate the "causing" limitation of the patent. As the Federal Circuit has explained, "the 'all limitations' rule restricts the doctrine of equivalents by preventing its application when doing so would vitiate a claim limitation." *Primos, Inc. v. Hunter's Specialties, Inc.*, 451 F.3d 841, 850 (Fed. Cir. 2006); *see also, Warner-Jenkinson*, 520 U.S. at 29 ("It is important to ensure that the application of the doctrine, even as to an individual element, is not allowed such broad play as to effectively eliminate that element in its entirety."). "Thus, if a court determines that a finding of infringement under the doctrine of equivalents would entirely vitiate a particular claimed element, then the court should rule that there is no infringement under the doctrine of equivalents." *Lockheed Martin Corp. v. Space Sys./Loral, Inc.*, 324 F.3d 1308, 1321 (Fed. Cir. 2003) (internal quotation omitted). Accordingly, Symantec has failed to raise a genuine issue of material fact with respect to whether CA has induced infringement under § 271(b).

Thus, the Court should conclude that Symantec has failed to raise a genuine issue of material fact with respect to whether (a) the EAV and ARCserve products screen data while it is being transferred or while the computer is receiving the data, and (b) the EAV products cause a quantity

of digital data to be transferred. Accordingly, the Court should grant CA's motion for summary judgment of no infringement with respect to the accused EAV and ARCserve products.[5]

F. *Content Inspection Products*

In its second motion, CA contends that it is entitled to summary judgement of non-infringement with respect to its Content Inspection products. For the reasons that follow, the Court should conclude that Symantec has raised genuine issues of material fact with respect to whether the Content Inspection products infringe the patent, both literally and by equivalents.

1. *The Accused Products*

CA's Content Inspection products fall into two categories. The first category, referred to as GIE, functions as a gateway between a wide area network, such as the Internet or an office network, and individual computer systems. Under this system, the network receives digital data from a source storage medium, and in turn transfers the data to the GIE. *See* CA's Content Inspection Br., Ex. 3, Decl. of Benjamin Goldberg, ¶ 32. The second category consists of the "plug-in" products MS-PIE, NS-PIE, and CVP. These programs do not themselves provide gateway functionality as the GIE program does, but rather work in conjunction with other programs that provide such functionality. *See id*., ¶ 33.[6] Professor Goldberg collectively refers to both GIE and to the third-party/plug-in combination as the Gateway Product. *See id*., ¶ 35. Goldberg states that the Gateway Product software runs on a computer system (or systems) and serves as a proxy between a client computer and a remote computer system. *See id*., ¶ 36. In the typical scenario, the client computer will request

---

[5]This conclusion renders it unnecessary to consider the other limitations of the patent claims which CA contends are not met by the EAV and ARCserve products.

[6]Specifically, MS-PIE works in conjunction with a Microsoft gateway product, NS-PIE operates in conjunction with a Netscape product, and CVP operates in conjunction with a Checkpoint product. *See id*., ¶ 34.

data from the Gateway Product, which in turn requests the data from the remote computer system. The remote system then transfers the data to the computer running the Gateway Product, which in turn transfers the data to the client computer. *See id*., ¶¶ 37-38. According to Professor Goldberg, the Gateway Products do not scan the transferred data until it has been written to the gateway computer's storage medium. *See id*., ¶ 40. Further, the client computer–that is, the computer having the destination storage medium–does not scan the data; rather the data is screened by the gateway computer and, if virus free, transferred to the client computer which merely receives and stores the data without screening it. *See id*., ¶ 43. CA contends that the Content Inspection, or Gateway, products fail to embody a number of the limitations of the '776 patent.

2. *Literal Infringement*

CA first argues that the Content Inspection products do not "caus[e] a quantity of digital data . . . to be transferred to a computer system having a destination storage medium," as required by both independent Claim 1 and independent Claim 18 (and therefore as required by all of the dependent claims as well). CA contends that the Content Inspection products fail to satisfy this claim limitation for two reasons. First, the gateway programs do not themselves cause any digital data to be transferred; rather other software, such as a downloading or copying program, causes the transfer. According to Professor Goldberg:

> 39. Unlike the claimed invention, a gateway operates as a component of a network. While a gateway forwards incoming data to its addressed destination, [but] it does not cause data resident on a source storage medium to be transferred. A gateway, like a postal mail carrier delivering mail, may put addressed mail in a particular destination mailbox, but neither the gateway nor the mail carrier causes the mail to be sent from its sender to the destination mailbox.
>
> 40. A user may be able to command a downloading or copying program to transfer data from a source computer to the user's computer, there is no way for the user to command or request that the Gateway product initiate such a transfer. The only role of the Gateway products is to screen data that has already been transferred

to the gateway computer.

CA's Content Inspection Supp. Br., Ex. 13, Supp. Decl. of Benjamin Goldberg, ¶¶ 39-40. Second, CA argues that the Content Inspection programs do not cause the transfer of a quantity of digital data as taught in the patent because the programs transfer only virus-free data after the data has been scanned; data containing a virus is not transferred to the destination storage medium. *See id.*, ¶ 41. According to Goldberg, this fails to meet the patent limitations because "the claims require that the digital data be transferred to the destination computer whether or not it contains a virus." *Id*. Symantec responds that, under the Court's construction of "computer" and "computer system," the computer that runs the gateway product is itself a computer system.

In a similar vein, CA argues that the Content Inspection products do not "receive and screen the transferred digital data," "automatically caus[e] the screened digital data to be stored," or "simultaneously search[] for a plurality of virus signatures . . . while said computer is receiving a stream of digital data for storage on said storage medium." Each of these arguments is premised on the same general argument as the "causing" argument, that is, that each of these functions is performed on the gateway computer and not on the client computer which is the ultimate destination of the transferred data.

Symantec responds, however, that the gateway products operate on a gateway computer that is itself a "computer system" under the Court's claim construction even when considered apart from the client computer. Symantec argues that because each of the steps of the patent are performed on the gateway computer by the Content Inspection products, the products infringe the patent. Symantec's argument is well-taken, and the Court should therefore deny CA's motion for summary judgment. As Symantec points out, there is no dispute that the gateway computer is itself a

computer system as defined by this Court's claim construction. And, as a computer system, there is sufficient evidence to establish a genuine issue of material fact that the Content Inspection products, operating on the gateway computer, meets each of the elements of the patent claims upon which CA seeks summary judgment. For example Professor Goldberg, CA's own expert, avers that the gateway product "makes its own request for the data." CA's Content Inspection Supp. Br., Ex. 13, Supp. Decl. of Benjamin Goldberg, ¶ 30. Further, Goldberg avers that the gateway computer itself is a computer system, *see id*., ¶ 28, and that this computer system has its own storage medium. *See id*., ¶¶ 31-32. Finally, Professor Goldberg avers that, after screening, the gateway program automatically either deletes the infected data or stores the clean data on the gateway computer's storage medium. *See id*. ¶¶ 33-34; Symantec's Content Inspection Supp. Br., Ex. A, Supp. Decl. of David Klausner, ¶ 14.

CA contends that "[t]he Court's construction of the term "computer system" used in this claim element excludes intermediate, unattended servers or 'gateway' computers located between the source computer and the destination computer." CA's Content Inspection Supp. Br., at 11. The Court's construction only means, however, that the gateway cannot be considered a part of a single computer system with another individual personal computer or workstation. Nothing in the definition prohibits a gateway computer from itself being a complete "computer system" within the meaning of the patent. And there is evidence that the gateway computer running the Content Inspection products, considered on its own, is a "computer system," *i.e.*, a "single personal computer or workstation" which is comprised of "a bus to which are connected a central processing unit, random access memory, a serial port, and a data storage medium." Opinion & Order, dated 3/16/05, at 16-17; *see* CA's Content Inspection Supp. Br., Ex. 13, Supp. Decl. of Benjamin Goldberg, ¶ 28

("A Gateway Product is software that runs on a computer system, generally a dedicated gateway computer system . . . ."). In other words, if some steps of the patented method were performed on the gateway computer and some steps performed on the client computer the two could not, under the Court's claim construction, be aggregated into one computer system; nothing in the claim construction, however, precludes a finding of infringement if the gateway computer is itself a complete computer system which on its own performs each step of the claimed method.

CA also argues that although the gateway computer may have a storage medium, it is not the computer having the *destination* storage medium because the destination storage medium is the storage medium on the client computer. This argument, however, would require the Court to abandon its construction of "destination storage medium," which adopted CA's own proposed definition instead of that proposed by Symantec. As explained in the claim construction Order, Symantec argued that destination storage medium should be construed as "a computer storage medium that is the intended endpoint of the transfer of digital data." CA, on the other hand, advocated a definition which merely required that the destination storage medium be the "computer storage medium that is the target of the transfer of data as a result of the causing step," and the Court adopted this construction of "destination storage medium." *See* Opinion & Order, dated 3/16/05, at 18. Thus, it does not matter that the client computer is the intended endpoint of the transfer of digital data. If, in fact, the gateway computer itself causes a transfer of digital data to its storage medium, then the gateway computer's storage medium is the "destination storage medium" taught in the patent claims.

In short, there remains a genuine issue of material fact with respect to whether the gateway computer is itself a separate computer system having a destination storage medium, and if so

whether the Content Inspection products operating on that gateway computer embody each limitation of the patent claims. Thus, there remains genuine issues of material fact with respect to whether the Content Inspection products literally infringe the '776 patent, and the Court should therefore deny CA's motion for summary judgment.

3. *Equivalents*

Further, even if there were no genuine issue of material fact with respect to literal infringement, CA's motion should nevertheless be denied because there remain genuine issues of material fact with respect to whether the Content Inspection products infringe under the doctrine of equivalents. As noted above, even if an accused product does not literally infringe the patent claims it may nonetheless infringe if it contains equivalents to each of the claim limitations. Under the doctrine of equivalents, "[a]n element is equivalent if the differences between the element and the claim limitation are 'insubstantial,'" *Zelinski v. Brunswick Corp.*, 185 F.3d 1311, 1316 (Fed. Cir. 1999); *see also*, *Ecolab, Inc. v. Environchem, Inc.*, 264 F.3d 1358, 1371-72 (Fed. Cir. 2001), a determination based on "whether the element performs substantially the same function in substantially the same way to obtain substantially the same result as the claim limitation." *Zelinski*, 185 F.3d at 1316-17 (citing *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 608 (1950)). Whether an element of an accused device is an equivalent, and thus infringes, is a question of fact for the jury. *See J & M Corp. v. Harley-Davidson, Inc.*, 269 F.3d 1360, 1366 (Fed. Cir. 2001).

Symantec argues that, when operating the Content Inspection products, the gateway computer serves as a proxy, or agent, of the client computer, *see* CA's Content Inspection Supp. Br., Ex. 13, Supp. Decl. of Benjamin Goldberg, ¶¶ 28-30, and that this client/proxy combination is equivalent to the "computer system" described in the patent. Symantec also argues that there is no

dispute that the client/proxy combination together performs all of the steps of the patent claims. CA advances several arguments as to why the client/proxy combination cannot be found to be equivalent as a matter of law, each of which is unavailing.

First, CA argues that the Court's construction of "computer system" to exclude intermediate gateway computers precludes a finding of equivalence. This argument is without merit. Even if gateway computers are excluded from the definition of "computer system," that alone says nothing about whether the gateway/client combination is *equivalent* to a "computer system." The whole point of the doctrine of equivalents is to consider elements which do not literally infringe the patent. CA's argument would do away with the doctrine of equivalents by prohibiting its application anytime there is no literal infringement. The question here is not whether gateway computers are equivalent to "destination computers," but whether the gateway/client combination is the functional equivalent of the "computer system" described in the patent claims. Importantly, the fact that the method of the accused product requires more steps than the claims asserted in the patent does not preclude a finding of equivalence. As the Federal Circuit has explained, in the context of a method claim "[e]quivalence is not defeated by using an additional step to achieve what the patentee does in one step." *EMI Group N.A., Inc. v. Intel Corp.*, 157 F.3d 887, 896 (Fed. Cir. 1998); *see also, Intel Corp. v. United States Int'l Trade Comm'n*, 946 F.2d 887, 896 (Fed. Cir. 1991); *cf. Schumer v. Laboratory Computer Sys., Inc.*, 308 F.3d 1304, 1312 (Fed. Cir. 2002) (a method claim which is "not tied to a particular device . . . must be interpreted to cover any process that performs the method steps.").

CA also argues that Symantec is estopped from arguing that the gateway/client combination is equivalent to the computer system described in the patent because of statements made during the

prosecution of the '776 patent. Specifically, in response to the examiner's initial rejection of the patent, the inventors stated:

> To prevent the spread of computer viruses using the art of record the user must remember to perform two steps. First, the user must remember to scan the source medium before initiating the data transfer. Second, after the source medium has been scanned, the user must initiate the data transfer from the scanned source to the destination medium.
>
> In contrast, the Applicants' invention requires only one step. The user simply initiates the data transfer. The program automatically screens the data, as it is being transferred and automatically inhibits the storage if a virus sequence is detected. The art of record does not operate in this manner.

CA's Claim Construction Br., Ex. 15, Amendment filed 8/26/92, at 5. The Court should conclude that this argument does not create an estoppel.

As the Federal Circuit has explained, "[p]rosecution history estoppel can prevent a patentee from relying on the doctrine of equivalents when the patentee relinquishes subject matter during the prosecution of the patent, either by amendment or argument." *Aquatex Indus., Inc. v. Techniche Solutions*, 419 F.3d 1374, 1382 (Fed. Cir. 2005). However, estoppel by amendment and estoppel by argument are not analyzed identically. When an amendment is made to the patent claims to overcome the examiner's objection, the court must "presume that the patentee surrendered all subject matter between the broader and the narrower language." *Festo Corp.*, 535 U.S. at 739. No such presumption arises, however, from a patent applicant's mere arguments to the examiner. As the Federal Circuit has recently explained, "[u]nlike amendment-based estoppel, we do not presume a patentee's arguments to surrender an entire field of equivalents through simple arguments and explanations to the patent examiner. Though arguments to the examiner may have the same effect, they do not always evidence the same clear disavowal of scope that a formal amendment to the claim would have." *Conoco, Inc. v. Energy & Envtl. Int'l, L.C.*, ___ F.3d ___, ___, 2006 WL 2372016,

at *12 (Fed. Cir. Aug. 17, 2006). Thus, estoppel by argument arises only if the applicant "clearly and unmistakably surrenders subject matter by arguments made to an examiner." *Aquatex Indus.*, 419 F.3d at 1382 (internal quotation omitted); *accord Deering Precision Instruments, LLC v. Vector Distrib. Sys., Inc.*, 347 F.3d 1314, 1324 (Fed. Cir. 2003).

Here, the patentees' argument to the examiner does not "clearly and unmistakably" surrender subject matter related to the "computer system" issue, or to the number of steps that the program itself must perform. It is clear that the statements to the examiner concerned the number of steps a *user* of the programs must perform, not the number of steps that the program itself performed. Even if the statements were sufficient to surrender some subject matter, the only subject matter which could reasonably be viewed as having been surrendered is a program which requires the user to do more than simply initiate the data transfer. Symantec's equivalence argument does not require more than one step on the part of the user; even using the gateway/client combination, the user still performs only one step. Thus, no estoppel by argument arises with respect to Symantec's equivalence argument.

Finally, CA argues that Symantec is estopped from arguing equivalence because Symantec's expert, David Klausner, gave only a conclusory statement regarding equivalence in his expert report and any further supplementation of that report would be unfair, as CA has already taken Klausner's deposition. Even if this were true, however, Symantec's equivalence argument with respect to the Content Inspection products is based entirely on Professor Goldberg's declarations and the actual statements made by Klausner in his expert report. Thus, this estoppel argument is without merit. Accordingly, the Court should conclude that Symantec has raised genuine issues of material fact with respect to whether the Content Inspection products infringe the '776 patent under the doctrine

of equivalents.

G. *Intrusion Detection Product*

Finally, CA argues that it is entitled to summary judgment with respect to its Intrusion Detection product. The Court should grant CA's motion with respect to this accused product.

1. *The Accused Product*

CA describes its Intrusion Detection product as a "packet sniffer" which can detect a virus and report that it has detected a virus, but which cannot itself affect the storage of data. According to CA, a packet sniffer on a network is akin to an eavesdropper – it can observe what's being said but cannot prevent it from reaching the intended recipient. *See* CA's Intrusion Detection Br., Ex. 3, Decl. of Professor Benjamin Goldberg, ¶ 62. According to CA's expert,

> Intrusion Detection examines data packets flowing across its network, but has no ability to inhibit the flow of any packet that it sees. When Intrusion Detection inspects files transferred across a network for virus signatures, it does so only after the entire file has been transferred to, and becomes physically present on, the destination storage medium. In other words, Intrusion Detection waits until it has seen all the data from an entire file go by before performing the screening. Moreover, although Intrusion Detection can see data transmitted between any of the computer systems and the gateway, and can affect future network events by sending its own packets out over the network, it has no capability for causing or inhibiting the storage of screened data on the destination storage medium.

Id., ¶ 63. CA contends, based on this description, that the Intrusion Detection program fails to meet a number of limitations of independent Claim 1 and dependent claims 6, 10-11, 13-14, and 16-17.

The Court need not consider each of the separate bases upon which CA contends its product does not infringe the patent because Symantec has failed to establish a genuine issue of material fact with respect to whether Intrusion Detection screens the incoming data "prior to storage on the destination storage medium" and thereafter "automatically inhibit[s] the screened digital data from being stored," and with respect to whether the programs "causes a quantity of digital data to be

transferred."

2. *"Prior to Storage" and "Automatically Inhibiting Storage"*

As reflected in the Court's claim construction, the first claim limitation requires that the data be screened "before the incoming digital data is sufficiently present on the destination storage medium and accessible by the operating system or other programs so that any viruses contained in the data can spread and infect the computer system/ Opinion and Order, dated 3/16/05, at 35. Professor Goldberg opines in his declaration that "[w]hen Intrusion Detection inspects files transferred across a network for virus signatures, it does so only after the entire file has been transferred to, and becomes physically present on, the destination storage medium." CA's Intrusion Detection Br., Ex. 3, ¶ 63; *see also*, CA's Intrusion Detection Supp. Br., Ex. 17, Supp. Decl. of Benjamin Goldberg, ¶ 66. CA also relies on the testimony of David Klausner, Symantec's expert, who in part testified:

Q: Now, isn't Intrusion Detection a sniffer?
A: What do you mean by "sniffer"?
Q: You're not familiar with that term?
A: I have an understanding, but you asked the question. So what do you mean by sniffer?
Q: What's your understanding of sniffer?
A: Something that examines what goes – what passes by without altering it.
Q: Isn't Intrusion Detection a sniffer?
A: It is by my definition.

CA's Intrusion Detection Br., Ex. 4, Dep. Tr. of David Klausner, at 195. Subsequently, Klausner testified:

Q: . . . . You talk about FTP – FTP, HTTP, and telnet. Let's focus on those and take them one at a time.

If you do an FTP download on your client computer and the file that you download contains a virus, will Intrusion Detection do anything to block that?
A: Not the way it's configured.

Q: Not in any way it can be configured, right?
A: That's what I meant.
Q: Okay. Now let's take HTTP. In an HTTP environment, if you download an HTTP pate that contains a virus, can – will Intrusion Detection do anything at all to block the download of that virus? It won't, will it?
A: It – it will not block a virus.
Q: And that virus can be stored on the destination storage medium, right?
A: That's correct.
Q: The same thing with telnet, right, a telnet session?
A: Yes, that's correct with telnet.

Id. at 196-97. CA argues that these statements from Goldberg and Klausner establish that the Intrusion Detection product neither screens data prior to storage on the destination storage medium, nor automatically inhibits the storage of the data if a predefined sequence is found.

Symantec argues that CA's own promotional materials–in particular the Intrusion Detection Administrator Guide–belie CA's claim. Except for the blocking feature discussed more fully below, nothing in the Administrator Guide contradicts CA's position here as it relates to the "prior to storage" and "automatically inhibiting storage" limitations of the patent claims. For example, the Guide lists as one feature of the program "[a] virus-scanning engine [which] detects network traffic containing computer viruses. It protects users from innocuously downloading virus-infected files." *See* Symantec's Intrusion Detection Br., Ex. 1, at 1-1 (Bates number CAI0013131). Nothing in that simple statement, however, suggests the means by which the software performs this function.

Symantec also argues that the Intrusion Detection "block it" feature performs all of the steps claimed in the patent. There is no dispute that a user running the Intrusion Detection software can create a blocking rule by selecting the action "Block It." *See id*. at 4-24 (Bates number CAI0013182). According to Klausner, this blocking action can be applied to the rule "match string in content," *see* Symantec's Intrusion Detection Br., Ex. 11, which in effect means that the program is screening data prior to storage. However, nothing in Klausner's report or declaration, or in any

other evidence submitted by Symantec, contradicts Goldberg's assertion that even in this mode of operation the screened packet of data "will make its way to its destination for storage or other disposition." *See* CA's Intrusion Detection Supp. Br., Ex. 17, Supp. Decl. of Benjamin Goldberg, ¶ 68. In other words, "while Intrusion Detection can affect future network events by sending its own packets out over the network, any data seen by Intrusion Detection will have also arrived at its destination," *id*., and Klausner's description of the blocking feature does not contradict this point. Likewise, Symantec's argument that the program's method of preventing Yahoo Messenger service fails to refute Goldberg's declaration that, even in this mode, Intrusion Detection does not inhibit the storage of the screened data. *See* CA's Intrusion Detection Br., Ex. 3, Decl. of Benjamin Goldberg, ¶ 68.

Symantec also relies on Klausner's testing protocol in which he set up the Intrusion Detection program to block an FTP download. In his declaration Klausner explains that he set up the program to block the EICAR (Europeans Institute for Computer Anti-Virus Research) string:

> I used eTrust Intrusion Detection version 2.0.0.10 to perform this blocking example. In the first screen shot, I selected the "Intrusion Attempt Detection Rules." This selection resulted in the second screen shot being displayed. At this second screen, I selected "FTP Block." I then selected "All FTP sessions" displayed in the third screen shot. At this third screen, I selected "Properties," which caused the fourth screen shot to appear. At this fourth screen shot, I selected "Match string in content." Note at the bottom of this screen shot that "Block action can be applied to this Rule Type Criteria." I then entered the eicar test string in the "Enter new string" field shown in the fifth screen shot. Note that multiple strings can be entered in this field. As seen in the sixth screen shot, the action "Block+Log" is selected.

Symantec's Instruction Detection Br., Ex. 12, Decl. of David Klausner, ¶ 35 & Ex. B. Klausner then avers that, after defining this rule, he attempted to download the eicar test string using the FTP protocol, but that the transfer was blocked. *See id*. at ¶ 36 & Ex. B (screen shot 7). This test, however, fails to raise a genuine issue of material fact for two reasons.

First, the declaration directly contradicts Klausner's deposition testimony, in which he unequivocally stated that Intrusion Detection will not block a virus string in an FTP download either in the way the program is configured or in any way that the program could be configured. *See* CA's Intrusion Detection Br., Ex. 4, Dep. Tr. of David Klausner, at 196-97. It is well established that a party may not create a genuine issue of fact for trial by offering an the affidavit of a witness that contradicts the witness's prior sworn testimony. *See Peck v. Bridgeport Machines, Inc.*, 237 F.3d 614, 619 (6th Cir. 2001); *Reid v. Sears, Roebuck & Co.*, 790 F.2d 453, 460 (6th Cir. 1986). Second, even assuming that this portion of Klausner's declaration properly may be considered, it fails to raise a genuine issue of material fact because it fails to detail how the blocking action works. That is, Klausner does not opine that the blocking action works prior to the storage of the data on the destination storage medium as that phrase is used in the patent.[7] Accordingly, the Court should

---

[7]CA also argues that Klausner's description of his test only contradicts his testimony that Intrusion Detection could not in any way be configured to prevent storage of data from an FTP download; it does not contradict his statement that the program does not prevent detection as configured. There is no evidence that the steps taken by Klausner are in any way the normal operation of the system, or that the system is intended to be operated in that manner. Nor is there any evidence that the configuration used by Klausner is suggested by CA's marketing and operating materials. CA argues, therefore, that Klausner's testing does not establish a genuine issue of material fact. The Court need not reach this argument unless it concludes, contrary to the recommendation above, that Klausner's declaration may be relied upon to contradict his deposition testimony and that the declaration otherwise establishes a genuine issue of material fact. To the extent the Court does so, however, and thus needs to reach this issue, the Court should reject CA's argument.

It is true, as CA notes, that the fact "that a device is capable of being modified to operate in an infringing manner is not sufficient, by itself, to support a finding of infringement." *Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1330 (Fed. Cir. 2001); *see also, High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc.*, 49 F.3d 1551, 1555-56 (Fed. Cir. 1995). It is equally true, however, that a product is not non-infringing merely because its infringing use was neither intended nor described to users. *See Intel Corp. v. United States Int'l Trade Comm'n*, 946 F.2d 821, 832 (Fed. Cir. 1991). In *Fantasy Sports Properties, Inc. v. Sportsline.com, Inc.*, 287 F.3d 1108 (Fed. Cir. 2002), the court harmonized these principles in the computer software context. The court explained that infringement may be found notwithstanding the rule of *High Tech* and *Telemac*

conclude that Symantec has failed to raise a genuine issue of material fact with respect to both whether Intrusion Detection screens data prior to storage and whether the program automatically inhibits the storage of the screened data if a predefined sequence is found.[8]

3. *"Causing a Quantity of Digital Data . . . to Be Transferred"*

The Court should also conclude that Symantec has failed to establish a genuine issue of material fact with respect to whether the Intrusion Detection program "caus[es] a quantity of digital data resident on a source storage medium to be transferred to a computer system having a destination storage medium." The Court has construed this phrase to mean "effecting by command, authority, or force the transfer of digital data resident on a source storage medium to a personal computer or work station having a computer storage medium which is the target of the data as a result of the 'causing' step." Opinion & Order, dated 3/16/05, at 35. Professor Goldberg opines that Intrusion Detection does not cause a quantity of digital data to be transferred because it is an intermediate gateway which does not itself cause the transfer to the computer having the destination storage medium. *See* CA's Intrusion Detection Br., Ex. 3, Decl. of Benjamin Goldberg, ¶¶ 71-72. Likewise,

---

if, "although a user must activate the functions programmed into a piece of software by selecting those options, the user is only activating means that are *already present in the underlying software*." *Id*. at 1118 (emphasis in original). Alteration supporting a finding of non-infringement requires an alternation to the actual software code itself. *See id*. In other words, infringement may be found if "the code underlying [the program is] written in such a way as to enable a user of that software to utilize the function . . . without having to modify that code[,] . . . regardless whether that means is activated or utilized in any way." *Id*. Under this standard, if Klausner's test on the eicar string may be considered, and if it otherwise were sufficient to show infringement, the test is not the type of alteration of the Intrusion Detection product which would bring it within the rule of *High Tech* and *Telemac*.

[8]As noted above, Symantec is estopped from asserting any range of equivalents for the prior to storage limitation, and the Court therefore need not consider whether the Intrusion Detection product infringes under the doctrine of equivalents with respect to this limitation. With respect to the "automatically inhibiting" limitation, Symantec offers no specific argument as to equivalence.

Symantec's expert testified that the client computer, not the network server or gateway running the software, initiates the transfer of digital data. *See id*., Ex. 4, Dep. Tr. of David Klausner, at 193-94.

In its initial response, Symantec argued that CA's argument was meritless because it was based on an inappropriate construction of the phrase "computer system," which could include a network such as that on which Intrusion Detection operates. In its claim construction, however, the Court adopted CA's construction, defining "computer system" as a "personal computer or workstation," Opinion & Order, dated 3/16/05, at 16, 35, and explicitly excluded from this definition more complex systems such as interconnected or distributed systems and channel processors. *See id*. at 17. In its supplemental response, Symantec notes that by the admission of CA's expert the Intrusion Detection program is being used to screen "the data being transferred by some other program (such as a downloading or copying program)," CA's Intrusion Detection Supp. Br., Ex. 17, Supp. Decl. of Benjamin Goldberg, ¶ 62, and that CA markets its product as being used to "monitor network traffic, detect suspicious network activity and intrusion attacks in real time, and to block unwanted network activity quickly and easily." Symantec's Intrusion Detection Br., Ex. 1, Intrusion Detection Administrator Guide, at 1-1 (Bates number CAI0013131). Symantec argues that this constitutes inducement of infringement for which CA is liable under 35 U.S.C. § 271(b). The Court should disagree.

Under § 271, "[w]hoever actively induces infringement of a patent shall be liable as an infringer." 35 U.S.C. § 271(b). As explained above in connection with CA's EAV and ARCserve products, to establish inducement of infringement Symantec must show two elements: (1) direct infringement on the part of someone, *see Alloc*, 342 F.3d at 1374; *Epcon Gas Sys.*, 279 F.3d at 1033; *Met-Coil Sys.*, 803 F.2d at 687; and (2) knowledge of the patent and the actual intent to induce

infringement, *see Alloc*, 342 F.3d at 1374; *Young Dental Mfg.*, 891 F. Supp. at 1348. Here, Symantec has offered nothing to show that any third party has infringed the '776 patent through the use of Intrusion Detection. Symantec's inducement argument derives from Goldberg's admission that software used with Intrusion Detection cause such transfers to take place. This admission, however, does not establish that the "causing" step is performed by Intrusion Detection, rather than the additional software. Symantec's inducement argument can be sustained only if a separate program causing the transfer of data is an equivalent to the "causing" limitation of the patent, or if the entire network can be viewed as the equivalent of a "computer system." Such equivalence findings, however, would effectively vitiate the "causing" and "computer system" limitations of the patent. As the Federal Circuit has explained, "the 'all limitations' rule restricts the doctrine of equivalents by preventing its application when doing so would vitiate a claim limitation." *Primos, Inc. v. Hunter's Specialties, Inc.*, 451 F.3d 841, 850 (Fed. Cir. 2006); *see also, Warner-Jenkinson*, 520 U.S. at 29 ("It is important to ensure that the application of the doctrine, even as to an individual element, is not allowed such broad play as to effectively eliminate that element in its entirety."). "Thus, if a court determines that a finding of infringement under the doctrine of equivalents would entirely vitiate a particular claimed element, then the court should rule that there is no infringement under the doctrine of equivalents." *Lockheed Martin Corp. v. Space Sys./Loral, Inc.*, 324 F.3d 1308, 1321 (Fed. Cir. 2003) (internal quotation omitted).

In short, Symantec has presented no evidence that Intrusion Detection meets the limitation of causing a quantity of digital data to be transferred, or that its use with other software would render CA liable for inducing infringement. Accordingly, the Court should conclude that CA is entitled to summary judgment of non-infringement with respect to the accused Intrusion Detection product.

H. *Conclusion*

In view of the foregoing, the Court should:

(1) conclude that there are no genuine issues of material fact with respect to whether the accused EAV and ARCserve products screen the data while it is being transferred or while the computer is receiving the data, and that there are no genuine issues of material fact with respect to whether the EAV products cause a transfer of digital data. Accordingly, the Court should grant CA's motion for summary judgment of no infringement with respect to the accused EAV and ARCserve products (docket #118);

(2) conclude that Symantec has raised genuine issues of material fact with respect to whether the accused Content Inspection products infringe the patent both literally and under the doctrine of equivalents. Accordingly, the Court should deny CA's motion for summary judgment of non-infringement with respect to the Content Inspection products (docket #119); and

(3) conclude that there are no genuine issues of material fact with respect to whether the accused Intrusion Detection product screens data "prior to storage," "automatically inhibits the storage of data," or "causes a quantity of digital data to be transferred." Accordingly, the Court should grant CA's motion for summary judgment of non-infringement with respect to the Intrusion Detection product (docket #121).

III. NOTICE TO PARTIES REGARDING OBJECTIONS:

The parties to this action may object to and seek review of this Report and Recommendation, but are required to act within ten (10) days of service of a copy hereof as provided for in 28 U.S.C. § 636(b)(1) and E.D. Mich. LR 72.1(d)(2). Failure to file specific objections constitutes a waiver of any further right of appeal. *Thomas v. Arn*, 474 U.S. 140 (1985); *Howard v. Secretary of Health*

& Human Servs., 932 F.2d 505 (6th Cir. 1991); *United States v. Walters*, 638 F.2d 947 (6th Cir. 1981). Filing of objections which raise some issues but fail to raise others with specificity, will not preserve all the objections a party might have to this Report and Recommendation. *Willis v. Secretary of Health & Human Servs.*, 931 F.2d 390, 401 (6th Cir. 1991); *Smith v. Detroit Federation of Teachers Local 231*, 829 F.2d 1370, 1373 (6th Cir. 1987). Pursuant to E.D. Mich. LR 72.1(d)(2), a copy of any objections is to be served upon this Magistrate Judge.

Within ten (10) days of service of any objecting party's timely filed objections, the opposing party may file a response. The response shall be not more than five (5) pages in length unless by motion and order such page limit is extended by the Court. The response shall address specifically, and in the same order raised, each issue contained within the objections.

s/Paul J. Komives
PAUL J. KOMIVES
UNITED STATES MAGISTRATE JUDGE

Dated:8/31/06

The undersigned certifies that a copy of the foregoing order was served on the attorneys of record by electronic means or U.S. Mail on August 31, 2006.

s/Eddrey Butts
Case Manager